Naval War College

Newport, R.I.

A Systems Approach to Assessing the Vulnerabilities of U.S. Domestic Sea Ports to Acts of Sabotage and Terrorism

By
David C. Grohoski
MAJ, USA

A Paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Advanced Research Programs.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature David C. Grohoski

28 May 1996

Paper Directed By
John B. Hattendorf, D. Phil.
Chairman, Advanced Research Programs

Arthur R. Adkins
LTC Arthur A. Adkins Date
Faculty Advisor

28 May 96
CAPT Charles C. Beck Date
Faculty Advisor

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority: N/A	
3. Declassification/Downgrading Schedule: N/A	
4. Distribution/Availability of Report: UNLIMITED	
5. Name of Performing Organization: ADVANCED RESEARCH DEPARTMENT	
6. Office Symbol: 35	**7. Address:** NAVAL WAR COLLEGE, 686 CUSHING RD., NEWPORT, RI 02841-5010
8. Title A Systems Approach to Assessing the Vulnerabilities of U.S. Domestic Sea Ports to Acts of Sabotage and Terrorism	
9. Personal Authors: Major David C. Grohoski, U.S. Army	
10.Type of Report: Final	**11. Date of Report:** 28 May 1996
12.Page Count: 67	
13.Supplementary Notation: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Advanced Research. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.	
14. Ten key words that relate to your paper: Harbors, Ports, Terminals, Port Security, Threat, Vulnerability Assessment, Risk	

15.Abstract: The U.S. national security strategy provides for two, nearly simultaneous, major regional contingency (MRC) operations. The U.S. Armed Forces transport more than 85% of their required sustainment supplies by sea. Strategic mobility planners assume that U.S. port operations can support the required deployment schedule without experiencing degradation or damage. Given the inherent vulnerability of seaports in our free and open society, the real issue is to determine the extent to which the ports are vulnerable. No agency or armed service has clearly determined the degree of vulnerability of domestic ports and terminals. There is no existing methodology to accurately assess the overall vulnerability of a port, thus, the current, subjective evaluations fail to adequately analyze real-world vulnerability. This research systematically combines the individual components of port security assessment into one comprehensive approach that will aid commanders and port authorities in accurately identifying threat,vulnerability, and risk; thus, providing useful information with which to tailor port security operations. The primary focus is on the vulnerability assessment and prescribes two interrelated measures to enhance the accuracy and usefulness of a vulnerability assessment. The first measure provides recommended guidelines in the identification of critical assets. The second provides an objective, analytical method to assess the vulnerability of critical assets. The conclusion of this research is that a systems approach is required in order to accurately assess port security. The Department of Defense and the Department of Transportation, the two departments with key responsibilities for strategic mobility, must confirm or disprove the validity of the assumption concerning port security.

16.Distribution / Availability of Abstract: A	Unclassified	**Same As Rpt**	**DTIC Users**

18.Abstract Security Classification: UNCLASSIFIED

19.Name of Responsible Individual: Director, Advanced Research Department

20.Telephone: (401) 841-3304	**21.Office Symbol:** 35

Abstract of

A Systems Approach to Assessing the Vulnerability of U.S. Sea Ports to Acts of Sabotage and Terrorism

The U.S. national security strategy provides for two, nearly simultaneous, major regional contingency (MRC) operations. The U.S. Armed Forces transport more than 85% of their required sustainment supplies by sea. Strategic mobility planners *assume* that U.S. port operations can support the required deployment schedule without experiencing degradation or damage. Given the inherent vulnerability of seaports in our free and open society, the real issue is to determine the extent to which the ports are vulnerable. No agency or armed service has clearly determined the degree of vulnerability of domestic ports and terminals. There is no existing methodology to accurately assess the overall vulnerability of a port, thus the current, subjective evaluations fail to adequately analyze real-world vulnerability. This research systematically combines the individual components of port security assessment into one comprehensive approach that will aid commanders and port authorities in accurately identifying threat, vulnerability, and risk; thus, providing useful information with which to tailor port security operations. The primary focus is on the vulnerability assessment and prescribes two interrelated measures to enhance the accuracy and usefulness of a vulnerability assessment. The first measure provides recommended guidelines in the identification of critical assets. The second provides an objective, analytical method to assess the vulnerability of the critical assets. The conclusion of this research is that a systems approach is required in order to accurately assess port security. The Department of Defense and the Department of Transportation, the two departments with key responsibilities for strategic mobility, must confirm or disprove the validity of the assumption concerning port security.

Preface

For Want of a Bullet

For want of a bullet, the soldier was lost
For want of a soldier, the platoon was lost
For want of a platoon, the company was lost
For want of a company, the battle was lost
For want of a battle, the war was lost

You might ask, "Why didn't the soldier have a bullet?"
The answer is, "Because the port didn't have electricity."
Because the port didn't have electricity, the forklift didn't work.
Because the forklift didn't work, the ship was loaded by hand.
Because the ship was loaded by hand, the ship didn't sail when it was scheduled.
Because the ship didn't sail as scheduled, the ship arrived late.
Because the ship arrived late, ammunition wasn't sent to the front on time.
Because the ammunition wasn't sent to the front on time, the soldier ran out of bullets.
Because the soldier ran out of bullets, he was killed.

This research is designed to identify critical assets
which accomplish critical functions
to execute the port's mission:

Ensuring the uninterrupted transshipment
of supplies and equipment
to support the
warfighter!

Table of Contents

LIST OF FIGURES

Chapter 1

Introduction

The successful accomplishment of any major regional contingency (MRC) scenario requires the ability to project force in a theater of operations. The ability to project force is directly related to our ability to maintain deployment and sustainment operations from continental United States (CONUS) sea ports and terminals. MRC plans assume that sealift will transport 85% of all resupply and 95% of all ammunition to the theater of operations.[1] The Department of Defense (DoD) has underestimated some vulnerabilities in the CONUS theater of operations. DoD has focused on the out-of-CONUS (OCONUS) theater threat and neglected the operational aspects of a CONUS threat. Overall strategic success in any theater depends upon a clear understanding and appreciation of all significant vulnerabilities.

DoD established U.S. strategic mobility requirements in two major studies: The Mobility Requirements Study (MRS) in 1992 and the Bottom-Up Review (BUR) in 1993.[2] The MRS was updated in March 1995. These analyses of our strategic deployment requirements did not consider a CONUS threat and *assumed* that U.S. port operations would support the OCONUS theater commander-in chiefs' (CINCs') requirements without disruption.[3]

Given the inherent vulnerability of sea ports and terminals in our free and open society, the real issue is to determine the extent to which they are vulnerable. No agency or armed service has clearly determined the degree of vulnerability of domestic commercial and military ocean terminals.

The United States Coast Guard (USCG), U.S. Army, U.S. Navy, port authorities, and other agencies conduct port security assessments. Definitions (of threat, vulnerability, and

risk), methodologies used to determine vulnerability, and the means of communicating the results vary from agency to agency. Moreover, many agencies attempt to consolidate the components of the port security assessment which results in a haphazard, piece-meal product of limited value.

Poorly designed and incomplete port assessments result in an inefficient application of port security measures. In a period of fiscal constraint and force reductions, governmental agencies and private businesses must maximize all available resources. The security of the ports and the ability to support national defense emergencies demands a reevaluation of existing port and terminal security measures.

A systems approach dissects the port security assessment into three components: threat analysis, vulnerability assessment, and risk analysis. Threat and vulnerability are two distinct elements of security requiring individual analysis. Threat analysis examines potential adversaries, their capability to disrupt port operations, and the likelihood of hostile action against a port. Vulnerability assessment determines the critical functions necessary to accomplish the port mission, identifies those assets required to complete critical functions, and then determines the vulnerability of each critical asset. Risk analysis is the component of a port security assessment that binds the process together. Risk analysis uses threat analysis and vulnerability assessment to determine the minimum level of security for assets. This approach provides useful information to commanders and port authorities and allows them to allocate limited resources to safeguard critical functions and, thus, accomplish the port mission (the transshipment of cargoes).

Organization and Content

This research is primarily concerned with the emergency deployment of military units and equipment from their peacetime locations through designated surface ports of embarkation (SPOE) to meet the required delivery date (RDD) in a military theater of operations. A major regional contingency (MRC) scenario would challenge agencies to provide uninterrupted port operations and could impugn those port security forces which have not conducted advance planning.

Following this introduction, chapter two provides a narrative description of the missions, responsibilities, and relationships of the agencies tasked with peacetime and mobilization port security operations. This research identifies the conflicting responsibilities associated with port and terminal security and recommends a single proponent agency to coordinate and direct the security efforts of all tenant activities.

The third chapter addresses the ways that port security relates to threat analysis. This study illuminates the fact that no intelligence agency currently provides threat analysis for the ports and highlights the inability of the ports to proactively tailor security measures commensurate with the threat situation. This research recommends that the U.S. Coast Guard (USCG) provide a port-specific threat analysis and disseminate timely intelligence products to the ports.

The fourth chapter proposes a methodology to assess the overall vulnerability of a port. The current approach to assessing vulnerability is inadequate because of its focus on facilities rather than assets. Since adversaries target specific assets and security measures safeguard assets, the focus of a vulnerability assessment should also address those assets that accomplish

critical functions in support of the port mission. This research provides a recommended outline for use in developing the vulnerability assessment. It also describes, in detail, the overall physical environment of the port, providing recommended guidelines and a checklist to assist in the identification of critical assets. Lastly, this study provides an objective, analytical method to assess the vulnerability of critical assets.

The fifth chapter addresses the ways that port security relates to risk analysis. Responsible agencies fail to conduct risk analysis on the ports, resulting in an inefficient and random application of security measures. This research recommends modifying the U.S. Army risk analysis model and uniformly conducting risk analysis for all U.S. strategic ports.

The sixth chapter provides recommendations to port commanders and port authorities for improving the preparedness of the sea ports to respond to potential hostile acts. The seventh chapter provides concluding thoughts.

Use of the Information

This research is intended to enhance port readiness and to facilitate communication, coordination, and cooperation among the agencies tasked with implementing security plans for strategic ports. The information in the study is intended primarily for use at the local level by the USCG Captain of the Port (COTP), port commander, or port authority. By providing a common body of information addressing all components of port security assessment, this research allows each port commander or port authority to best align his/her operations and resources for the efficient and secure accomplishment of the mission.

---

[1] U.S. Department of Defense, Joint Chiefs of Staff, Mobility Requirements Study, Bottom-Up Review Update, (Washington: 1995), D-5.
[2] U.S. Department of Defense, Report on the Bottom-Up Review, (Washington: 1993), 1-109.
[3] U.S. Department of Defense, Joint Chiefs of Staff, Mobility Requirements Study, Bottom-Up Review Update, (Washington: 1995), IV-A-5.

Chapter 2

Port Security Responsibilities

General

According to the Code of Federal Regulation (CFR), "owners and operators of vessels or waterfront facilities have the primary responsibility for protecting and securing their property... [and] to take all necessary precautions for protection against sabotage and other subversive acts."[1] The regulation, however, fails to identify an agency responsible for ensuring compliance with the directive. There is no statute or regulation which *clearly* assigns overall responsibility for port security to one agency.

Port authorities, private businesses, and governmental agencies devote their attention and resources toward addressing security concerns within the narrow scope of their individual operations. This piecemeal approach to addressing port security fails to maximize available resources. No one agency assesses the threats, vulnerabilities, and risks associated with the total port operation (waterside and shoreside) and no agency attempts to synergistically coordinate appropriate and effective security measures. DoD and the Department of Transportation (DoT), the two principal departments with key transportation responsibilities in support of national defense emergencies, need to identify a single proponent for port security and empower that agency to coordinate the efforts required to ensure adequate port security.

In January 1985, six Federal agencies, within DoD and DoT, signed the Memorandum of Understanding (MOU) on Port Readiness. The MOU was developed to "ensure military and commercial port readiness [will] support deployment of military personnel and cargo in the

event of a national defense contingency."[2] In 1988, a seventh organization, the Maritime Defense Zone (MDZ), signed the MOU. The MOU establishes peacetime requirements, outlines signatory agencies' responsibilities, facilitates inter-agency communication, promotes the best use of personnel and resources, and establishes local Port Readiness Committees (PRCs). While the MOU charges the U.S. Coast Guard with responsibility for port security, it assigns functional responsibilities for security among the signatory agencies.[3]

The seven signatory agencies include: the U.S. Army Corps of Engineers (USACE), the U.S. Army Military Traffic Management Command (MTMC), the U.S. Coast Guard (USCG), the Maritime Administration (MARAD), the U.S. Naval Control of Shipping Organization (NCSORG), and the U.S. Maritime Defense Zone (MDZ). The MOU establishes the National Port Readiness Steering Group (NPRSG) and the National Port Readiness Working Group (NPRWG). The NPRSG provides policy direction and sets broad priorities for accomplishing the objectives set out in the MOU. The NPRWG is responsible for implementing policies and priorities set by the steering group. The MOU also recommended the creation of local Port Readiness Committees (PRCs) to enlist multi-agency support of the overall program. Collectively, the NPRSG, NPRWG, and the PRCs comprise the National Port Readiness Network (NPRN). The composition of the organizations includes representatives from the signatory agencies. Other governmental agencies, non-governmental organizations, and private businesses may participate in the NPRN (at the national and local levels) but cannot establish policy direction and priorities.

Port and terminal security is a shared responsibility among federal, state, and local government agencies as well as the involvement of private businesses. Although sea port and

terminal operations involve many agencies, this analysis primarily addresses the signatory agencies.

Signatory Agency Responsibilities

U.S. Army Corps of Engineers (USACE)

USACE constructs, operates, and maintains navigation projects in ports and waterways (e.g., channels, locks, dams, etc.). From a port security standpoint, USACE provides the resources to remediate channel obstructions and keep the lanes open for vessel traffic.

Military Traffic Management Command (MTMC)

MTMC, a component of the U.S. Transportation Command (USTRANSCOM), coordinates force movement to seaports, prepares the ports for ships and cargo, and supervises the loading and offloading operations at ports. MTMC designates a major port command (MPC) to plan, coordinate, and control MTMC operations at each strategic port. MTMC relies on augmentation from the Reserve Component to operate ports and terminals in times of national emergency, including Port Security Companies which augment existing port security elements. In accordance with the MOU on Port Readiness, MTMC is also the proponent for shoreside security operations.

U.S. Coast Guard (USCG)

The USCG, an agency within DoT, is responsible for the security all U.S. ports (i.e. waterside security). The Coast Guard is tasked to develop emergency response plans both as a federal law enforcement agency and as a military service to meet national mobilization requirements.[4] The local USCG Marine Safety Office (and its higher counterpart, the Office of Marine Safety, Security and Environmental Protection) is tasked with ensuring the safe

movement of vessels and cargoes in the port environment, the prevention of accidents during transportation of dangerous cargoes, and the prevention of willful acts of sabotage and terrorism.[5]

The USCG assigns a senior officer as the Captain of the Port (COTP) for each major U.S. port. The COTP has a lead role in ensuring that adequate security is maintained to safeguard vessels, waterfront facilities, and harbors within his/her jurisdiction. As such, the COTP is responsible for providing waterside security for essential port facilities and maritime assets. Landside security, particularly as it pertains to landward approaches to facility property, falls primarily to the owner/operator of the vessel or facility and state and municipal law enforcement agencies.

During a national emergency or mobilization, the USCG may be transferred to the Department of the Navy. Under such circumstances, its responsibilities include: continuation of peacetime statutory functions, intensification of peacetime operations critical to national defense operations, and national defense operations (e.g., coastal/harbor defense, port security, surveillance and interdiction, providing aids to navigation, search and rescue, enforcement of U.S. laws and treaties, and commercial vessel safety).

Maritime Administration (MARAD)

MARAD, another agency within DoT, provides ships to meet DoD requirements in times of national defense emergencies. Specifically, MARAD coordinates the use of commercial shipping services, containers, and port facilities and services for use by defense agencies. MARAD also manages and maintains the National Defense Reserve Fleet (NDRF).

MARAD's role in port security operations is limited to coordinating resources for use by DoD agencies.

Military Sealift Command (MSC)

MSC, a component of USTRANSCOM, provides strategic sealift for the support and sustainment of military forces wherever needed. It is the single manager of ocean transportation for strategic mobility, providing worldwide logistical sealift services for all elements of DoD. MSC relies on its Strategic Sealift Force of government-owned and chartered U.S. flagged ships to provide ocean transportation. In accordance with the MOU on Port Readiness, MSC is the proponent responsible for onboard ocean vessel security operations.

Naval Control of Shipping Organization (NCSORG)

NCSORG is a U.S. Navy Reserve element that ensures the safe movement of merchant shipping during a national defense emergency. In accordance with the MOU on Port Readiness, NCSORG is concerned with ocean vessel security as it relates to convoy marshaling.

Maritime Defense Zones (MDZ)

MDZs are U.S. Navy Third Echelon commands within the fleet CINC organization. In peacetime, MDZ commanders conduct planning and exercises of Naval Coastal Warfare (NCW). When activated, MDZ commanders assume operational control for NCW within their areas of responsibility. In accordance with the MOU on Port Readiness, MDZs conduct defense operations (e.g., port security, harbor defense, and coastal defense) in order to maintain control of vital sea areas.

Single Agency Security Proponent

Among the signatory agencies, the USCG and MTMC play lead roles in port security. MTMC primarily addresses shoreside security concerns during the conduct of military outloads. With the exception of military ocean terminals, MTMC does not maintain daily contact with the port and is not involved with actual port functions until it commences deployment operations.

State and local port authorities, while not signatory agencies of the MOU, have a vested interest in the safety and security of their commercial port operations. The port authorities play an active role in the PRCs and work with the COTP to ensure compliance with DoT regulations. Most port authorities lack the resources to expand the scope of their security responsibilities.

The USCG already plays a lead role in port security, the authority of the COTP should be expanded to encompass shoreside security for the following reasons: (1) the USCG is best suited to address port security issues both as a federal law enforcement agency and as a military service; (2) the USCG is an established member of the port community, respected by both military and civilian agencies; (3) as the chairperson of the local PRC, the COTP already provides guidance and direction toward the accomplishment of NPRN policies and is, therefore, able to expand the scope of his/her leadership within the port with minimal agitation to the autonomy of the port authority; (4) the USCG has similar peacetime and contingency responsibilities with an adequate force structure with which to respond to emergency response situations in the port and, with minimal force modification, could expand the scope of their

responsibilities; and (5) the USCG best understands port functions and is able to coordinate limited resources to safeguard critical assets.

Summary

No one agency is the overall proponent for port and terminal security. The security and defense of the nation's ports involves numerous organizations which are responsible for different aspects of port safety, security, and harbor defense. The USCG is responsible for the waterside threat. MTMC is responsible for those portions of terminal security associated with the military outload. The port authorities, as owners and operators, have security responsibilities associated with the port, terminals, and shipping. Nevertheless, there is not a clearly identified single, proponent for port and terminal security.

The Code of Federal Regulations and MOU on Port Readiness should *assign* overall responsibility for *all* aspects of port security to the USCG. The USCG already possesses the organizational structure at each U.S. strategic port to accept this mission. Additionally, the NPRN should direct the Port Readiness Committees to conduct accurate port security assessments in order to ensure port readiness in the event of a national defense emergency.

---

[1] "Protection and Security of Vessels, Harbors, and Waterfront Facilities," Code of Federal Regulations, Title 33--Navigation and Navigable Waters, (Washington: U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, 1 July 1995), Chap. I-70.
[2] U.S. Department of Transportation, Maritime Administration, Port Emergency Operations Handbook for Federal Port Controllers, (Washington: 1992), Appendix E.
[3] Ibid., Appendix E, C-1.
[4] "Protection and Security of Vessels, Harbors, and Waterfront Facilities," Code of Federal Regulations, Title 33--Navigation and Navigable Waters, (Washington: U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, 1 July 1995), Chap. I-70.
[5] U.S. Department of Transportation, United States Coast Guard, Marine Safety Manual; Volume VII, Port Security, (Washington: 1993), 1-1.

Chapter 3

Threat Analysis

General

In 1983, four Puerto Rican nationalists were indicted for bombing five military installations. In 1986, eight United Freedom Front members were indicted for bombing four Army and Navy Reserve centers.[1] In 1989, five environmental extremists were indicted for conducting sabotage at a nuclear power station. Libyan agents in 1987, members of the Syrian Social Nationalist Party in 1987, and Japanese Red Army members in 1988 were all captured before carrying out planned bombings in this country.[2] In spite of the Federal Bureau of Investigation's (FBI's) increased efforts, extremist organizations continue to pose an increasingly more dangerous threat.

In 1988, Oliver Revell, Executive Assistant Director for the FBI told a Senate Subcommittee that it is vital for the U.S. to "develop, implement, and maintain a national program which addresses potential and actual acts of terrorism directed against key assets of the infrastructure of our nation."[3] DoD identifies port facilities as *key* infrastructure *assets* which are required to support DoD mobilization, deployment, and sustainment efforts.[4] However, DoD does not provide any resources or analysis for identifying potential threats to key assets (e.g., ports). The USCG Intelligence Collection Center (ICC) provides threat assessments of limited value addressing, "foreign travel, port calls, and domestic security issues associated with USCG personnel."[5]

DoD and DoT, in conjunction with the NPRN, need to conduct threat analysis specifically addressing U.S. domestic seaports (i.e. port-specific threat analysis) for two primary reasons.

The first reason is that no intelligence agency considers or determines whether an adversarial group will target port assets. Threat analysis is an essential component of the port security assessment because it provides: an identification of potential threat groups, a determination of their capabilities, and an assessment of the likelihood that an adversary will target a port. The second reason for a port-specific threat analysis is to streamline the distribution of pertinent information to user-agencies (e.g., USCG, MTMC, etc.) who require the intelligence product. Effective port and terminal security is predicated on receiving timely and accurate threat intelligence summaries. Intelligence, when properly evaluated, allows port security elements to best employ their resources to prevent or minimize the impact of hostile acts against the port. Port security forces cannot adjust their security posture in a proactive manner without sufficient knowledge of a probable attack.

Threat Intelligence Collection

The intelligence community initially identifies threats to domestic seaports as part of its routine intelligence collection effort. The FBI is the lead agency responsible for all aspects of domestic terrorism and sabotage (e.g., identification, monitoring, etc.). The Central Intelligence Agency (CIA) collects information on foreign groups which pose threats to the U.S. The Defense Intelligence Agency (DIA) remains primarily focused on collecting, analyzing, and monitoring threat nations' armed forces and is expressly prohibited from collecting intelligence on U.S. citizens in the United States. The USCG ICC is a third party user of most intelligence products (i.e. the ICC does not have personnel in the field collecting information) and, therefore, does not receive many of the reports passed to, and produced by, the primary collecting agencies (e.g., FBI, CIA, etc.). Nevertheless, the ICC should increase

its communication and coordination with intelligence collection agencies and obtain information for use in developing port-specific threat analyses.

Threat Intelligence Analysis

Current threat analyses do not provide readily useful information to the seaports because there is no determination made concerning the likelihood of an attack against a port. Threat analysis is comprised of three components: organizations, capabilities, and likelihood. The first component is designed to identify potential threat organizations. The second component determines the capability of a threat organization to disrupt port operations. The third component assesses the likelihood that a threat organization will actually conduct a hostile act against a specific port.

Intelligence agencies adequately identify subversive groups and individuals and assess their capabilities. However, there is neither an established *method* by which to assess the likelihood that an adversarial group or individual may target a port, nor an *agency* to do so.

Threat Intelligence Dissemination

Intelligence collection agencies fail to adequately disseminate threat products to the government agencies required to safeguard assets. Agencies (e.g., USCG, MTMC, port authorities, etc.) who desire current threat summaries must request (i.e. "pull") specific information from the agencies who collect and analyze information. Commercial ports generally rely on the USCG ICC for threat information. The ICC transmits threat information to port activities through the local USCG offices. Most of the threat summaries provide overly broad and relatively useless compilations of world-wide threat information.

Intelligence agencies must improve dissemination of intelligence summaries to the federal, state, or local agency required to respond to the potential threat. Additionally, intelligence agencies must provide information that is specifically pertinent and useful to the ports.

Summary

DoD and DoT, in conjunction with the NPRN, should direct the USCG Intelligence Collection Center (ICC) to develop, implement, maintain, and disseminate a port-specific threat analysis. Additionally, the ICC should improve its communication and coordination with the FBI and other intelligence collection agencies in order to obtain current information on potential threats from which to analyze potential impact on specific ports.

An act of terrorism or sabotage tied to a military deployment could seriously affect the MRC plan or any deployment requiring sealift. The U.S. ports which deploy and sustain our armed forces present a lucrative target whose damage or destruction would enhance the prestige of any terrorist organization as well as seriously jeopardize the timely execution of the MRC plan. Timely and accurate port-specific threat analyses will allow commanders and port authorities to properly allocate resources to enhance overall port security.

---

[1] The United Freedom Front (UFF) is a left-wing, radical, domestic terrorist organization. The left-wing, in the U.S., is characterized by extreme egalitarianism, hatred of capitalism, and overt opposition to militarism. Recent leftist terror in the U.S. is attributed to holdovers from the student movements and radical prison reforms of the 1970s.

[2] Brent L. Smith, Terrorism in America: Pipe Bombs and Pipe Dreams, (New York: SUNY Press, 1994), 17-29.

[3] Oliver B. Revell, III, Statement, U.S. Congress, Senate Committee on Judiciary, Terrorist Attacks Against the United States, Hearings, (Washington: The U.S. Govt. Print. Offc., 1990), 5.

[4] U.S. Department of Defense, DoD Regulation 5160.54, Key Asset Protection Program, (Washington: U.S. Govt. Print. Offc., 1992), 2-1.

[5] U.S. Department of Transportation, United States Coast Guard, Marine Safety Manual; Volume VII, Port Security, (Washington: 1993), 5-9.

Chapter 4

Assets and Vulnerabilities

General

The U.S. Coast Guard manual on port security recognizes that, "while the number of domestic maritime terrorist or subversive acts have been few, the vulnerability of many U.S. ports is quite high."[1] The USCG, U.S. Navy, MTMC, port authorities, and others have requirements to determine the relative vulnerability of port *facilities*. However, all existing vulnerability assessment methodologies focus on factors which do not relate to the port mission (i.e., the transshipment of cargoes). None of the responsible agencies identify those *assets* which provide *critical functions* for accomplishing the port mission. Consequently, the current assessments fail to provide commanders and port authorities with useful information concerning the vulnerability of critical port assets, the loss or disruption of which could have a significant negative effect on U.S. warfighting or sustainment capabilities.

The USCG defines vulnerability as "the susceptibility of an *asset* to an adverse action through which its effectiveness is reduced or eliminated."[2] However, current vulnerability assessments focus almost exclusively on facilities and physical security analysis. To enhance usefulness to commanders and port authorities, the entire focus of the assessment must change from facilities to *assets*. Vulnerability assessments must determine the *critical functions* necessary to accomplish the port mission, identify those *assets* required to complete critical functions, and then determine the vulnerability of each *critical asset*.

There is no existing methodology to accurately assess the overall vulnerability of a port, and the current subjective evaluations fail to adequately analyze real-world vulnerability for

two principal reasons. First, there are no standardized guidelines to aid in identifying the critical assets of a port. Second, there is no objective method to assess the vulnerability of critical assets. Without carefully examining the vulnerability of individual critical assets, generic port vulnerability assessments present, at best, useless and, at worst, misleading information to commanders and port authorities.

This research recommends an outline for use in developing the vulnerability assessment. Additionally, this research prescribes two interrelated measures to enhance the accuracy and usefulness of a vulnerability assessment. The first measure provides a recommended checklist and guidelines to assist in the identification of critical assets. The second provides an objective, analytical method to assess the vulnerability of critical assets.

Procedures for Developing a Vulnerability Assessment

A port vulnerability assessment requires in-depth knowledge of intermodal transshipment operations, physical security, engineering, and other aspects of port operations. To ensure the accuracy of the assessment, the individual in charge of the assessment should assemble a team of subject matter experts before attempting to complete the vulnerability assessment. The vulnerability assessment is developed in paragraph format using the outline described in Appendix A (Vulnerability Assessment Outline).

The vulnerability assessment outline provides the steps in the overall assessment procedure: (1) request a current threat analysis from the appropriate agency; (2) obtain drawings, maps, and plans of the facilities to be studied; (3) obtain the port mission statement and determine the list of required functions; (4) prioritize the list; (5) determine the location of all facilities to be studied and type of construction; (6) study all aspects of the physical security plan; (7)

identify critical assets of the port and terminal; (8) review existing contingency and back-up plans relevant to the continuation of port/terminal operations; (9) conduct a site visit to discuss and evaluate vulnerabilities and plans to mitigate the adverse effects; (10) complete a vulnerability assessment worksheet for each critical asset; and (11) compile the information and provide recommendations and a summary.

Determining Critical Functions and Critical Assets

General: Critical functions will vary from port to port and from mission to mission. Only an analyst who understands the complexities of intermodal transshipment operations can accurately determine which assets provide functions that are critical to the port mission.

When diagnosing the potential vulnerabilities of a port, it is important to first consider the mission of the port and to identify those functions required to accomplish the mission. Second the analyst must identify the assets required to complete the critical functions. The third step involves determining those assets whose loss or damage, without an alternate or back-up, would hinder the execution of the port's mission. The third step results in a list of critical assets which warrants further analysis.

The transshipment of cargo is the single, primary mission of a port. All ports have certain common functions necessary to accomplish the port mission (e.g., wharf operations, cargo transfer, etc.). However, the mission of the port may require other, specific functions. For example, the Military Ocean Terminal at Sunny Point (MOTSU) performs the *transshipment of containerized ammunition* (the port mission). In addition to wharf operations and cargo transfer, "container restuffing" (i.e. preparing containers for transshipment) is a critical function for the accomplishment of MOTSU's mission. Only those functions which contribute

to accomplishing the port's primary mission constitute *critical functions*, any other functions are secondary in nature, or are in direct support of the primary function.

After identifying critical functions, the analyst determines the assets required to complete the critical functions. The analyst will examine components of the port as they relate to accomplishing functions. Many ports possess redundant systems or have alternate resources available to permit the continuation of vital functions even when one or more components experiences loss, damage, or degradation. Contingency planning can significantly decrease the criticality of any single asset. Terminals without back-up plans are susceptible to extended disruptions and delays. The following subsection provides a component checklist to assist in identifying critical assets within a port.

Component Checklist and Recommended Guidelines: The components contained in the checklist provide the analyst with a starting point from which to develop the critical asset list. The analyst must use his/her knowledge to properly identify those assets which accomplish a function which is critical to the port mission. Since the assessment is port-specific, the criticality of an asset may vary from port to port and from mission to mission. Much of the required information is contained within the port's master mobilization plan and is available from the port authority or USCG. Specific examples cited at the beginning of the component descriptions are intended to provide clarity and demonstrate interrelationships among the components.

Harbors: The Wilmington Harbor approach channel presents a critical asset for the Port of Wilmington, NC. The port possesses only one route in and out of the harbor. The criticality of this channel is underscored by the fact that the channel is relatively narrow, it suffers from a

heavy accumulation of silt which limits the controlling depth, there are numerous bends and turns along the isolated and remote 30 mile approach, and the channel is subject to tidal conditions which restrict larger draft vessels to transiting only at high tide.

A harbor is a "partially enclosed body of water, natural or artificial, which provides protection for vessels to load or unload."[3] Only when a harbor has been developed for transacting business between ship and shore does it become part of port. A port consists of a harbor plus terminal facilities. When analyzing potential vulnerabilities in the harbor area, it is important to note: (1) current harbor traffic information (e.g., volume of traffic in the harbor, monthly and annual tonnages, use by non-U.S. flag vessels, etc.); (2) specific concerns and limitations within the harbor (e.g., narrow width of the channel precluding the passing of vessels, limited width and depth of turning basins which necessitates the use of additional tugs, sharp turns and bends in the channel which slow vessel transit times, etc.); and the following subsections:

Harbor Works: Harbor works (e.g., breakwaters, jetties, groins, sea walls, bulkheads, dikes, and locks) provide shelter, control water flow, and regulate erosion necessary for maintaining the navigability of a harbor. Harbor works do not include port facilities that are designed specifically for the transfer of cargo and the servicing of ships. The analyst should address the type, location, alignment, dimensions, and construction design of all harbor works.

Channels: Fairways, or channels, provide the approach and entrance to the harbor. The analyst should: (1) provide the location, length, width, depth (indicate the particular reference plane, such as mean low water [MLW], when reporting depths), and configuration of all channels, passing lanes, etc.; (2) describe potential chokepoints which a scuttled or grounded

vessel could effectively block; (3) discuss the effects of shoaling and siltation; (4) provide information on the land along the banks of the channel (e.g., developed, undeveloped, sparsely inhabited, etc.) as well as islands and tributaries; (5) list any fairway with controlling dimensions that limit the size (draft, length, beam, or height above water) of ships that can traverse the channel; (6) provide the location, alignment, and radius of tightest turn; (7) identify the shortest tangent; (8) provide the controlling depth and width; and (9) describe the overhead clearance throughout the entire length of the channel (e.g., bridges, power lines, cables, etc.).

Anchorages: The term 'anchorage' refers to a designated area where a ship employs its own anchors while waiting to use the terminal facilities. Harbors frequently provide fixed moorings where space restrictions prohibit free-swinging anchorage, where the number of accommodations is limited, and where a more secure berth (than that provided by a ship's own anchors) is desired. Fixed moorings may consist of anchored buoys or mooring posts. The analyst should describe the details of all anchorages and moorings (e.g., location, diameter, depths, holding ground, protection afforded, number available, and constraints).

Ports: The U.S. Army Corps of Engineers (USACE) harbor maintenance equipment is a critical asset for the Port of Wilmington. The harbor maintenance equipment provides the means of ensuring channel navigability (e.g., dredging, salvage, etc.). Heavy siltation in the harbor requires constant dredging operations to maintain minimum channel depths. While USACE is responsible for maintaining the integrity of the port, the Wilmington Port Mobilization Master Plan states that, "the sinking, scuttling, or sabotage of a larger vessel, particularly in the 600 to 900 foot range, would present a major problem to navigation,

requiring extensive and time consuming salvage operations that would exceed the capabilities of USACE on-site assets and would stretch the capabilities of even the largest, most experienced firms, assuming they were available to do the work."[4]

A port is defined as "any zone contiguous to or a part of the traffic network of an ocean transportation system, military or civilian, within which facilities exist to transship persons and/or property between domestic carriers and coastal, intercoastal, and overseas carriers."[5] A port consists of a harbor and the corresponding waterway which links it to a water transportation route. It extends landward to include the berths, docks, wharves, piers, sea walls, and supporting waterfront facilities.

When analyzing ports it is important to note: (1) the facility construction and condition; (2) principal port activities; (3) estimated port capacity (metric tons per day); (4) the largest vessel that can be accommodated; (5) the depth and width of entrance channel approaches; (6) the depth, width, radius, and clearance of turning basins; (7) the depth, width, and clearance of alongside berths; (8) hydrographic conditions; (9) geophysical conditions; (10) the number, locations, types of buoys, dolphins, etc. for each class of berth (e.g., commercial, tanker, etc.); (11) all available harbor maintenance equipment (include the owner, location, number, capabilities, and types of equipment [e.g., dredging, salvage, barges, etc.] to ensure unobstructed channel transit); (12) all available tugs (include the owner, location, number, capabilities, and types of equipment [e.g., pusher, puller, etc.] to facilitate channel passage; and (11) aids to navigation (e.g., lighthouses, beacons, buoys, etc.).

Terminals: A terminal is that part of a port consisting of the shoreside components required to support port operations. Terminals extend inland to include support buildings,

staging areas, marshaling areas, warehouses, storage tanks, roads, railways, on-load/off-load equipment, and other assets required to operate a port.

When describing the terminal, the analyst should: (1) provide a general description of the terminal and facilities located outside the perimeter; (2) specify the size, layout, and configuration of the terminal complex; (3) describe the landside access to the terminal (e.g., pedestrian, train, vehicle, etc.); (4) describe the waterside access to the terminal, including inland waterway approaches; (5) identify storm drainage tunnels located beneath the ground surface that could be used as an infiltration route; (6) describe air access, to include the location, distance, and capabilities of the nearest airports; (7) describe any aircraft handling assets within the port complex, including open areas capable of supporting helicopters; (8) identify the perimeter fencing, gates with vehicle barriers, and other measures in place to restrict access; (9) discuss any legally restricted areas within the channel and approaches; (10) identify lighting for wharves, holding yards, and rail yards; and (11) any other concerns, constraints, or items of special interest associated with the terminal.

Wharves: The South Wharf is a critical asset for the Military Ocean Terminal at Sunny Point (MOTSU). The South Wharf is the only wharf which possesses container cranes used for the transshipment of containerized ammunition (the port's mission). The criticality of the wharf increases since there is no other DoD facility capable of replacing the function provided by this one wharf (i.e. MOTSU's South Wharf). The restricted controlling depth and absence of a usable turning basin prevents the use of the North Wharf.

Wharves provide the basis for on-loading/off-loading operations in a port. The term wharf is used in two ways. In its broader sense, a wharf is the general designation for all landing

structures, including piers. Specifically, a wharf is the type of structure that parallels the shoreline and provides berthage at its face only. A pier-type of structure projects into the water at an angle with the shoreline. Berthage is usually available on the two sides of a pier. The analyst should provide the following information on each wharf:

Construction: Wharf construction generally falls into one of two categories: open construction and solid construction. Open construction consists of open-spaced wooden piles which support a wooden deck; it is the least permanent form of wharf construction. Solid construction consists of a solid wall backed by fill with a solid surface decking. Solid construction usually includes concrete and steel piles or quays with a reinforced concrete deck. The type and condition of the deck surface has an important bearing on the utility of a wharf (e.g., the ability to support the wharf railroad and other access roads).

Dimensions: The analyst must precisely measure all sides of the wharf since all sides may not be equal. Additionally, useable berthing space may or may not coincide with the overall length; shoals or other obstructions may decrease the usable length of a wharf.

Capacity: The analyst must determine the capacity of each wharf and identify any special or unusual berthing conditions (e.g. the breasting of ships off the wharf by means of pontoons, draft limitations, etc.). The analyst should also identify the primary and secondary wharves in order to determine whether or not the terminal possesses a more critical wharf.

When determining the criticality of the wharves the analyst should address: the number, normal use (e.g., general cargo, bulk cargo, supplementary, principal, etc.), construction, location, linear measurement, depth alongside, height of the deck, standard berth class, clearance, available utilities, and constraints.

Transportation Systems: The bridges constitute critical assets for the Blount Island Terminal in the Port of Jacksonville, FL. As the name implies, the terminal is situated on an island that requires the use of bridges for both road and rail traffic to gain access to the terminal. All cargoes and support personnel must transit the bridges to ensure uninterrupted port operations. Damage to or destruction of the bridges would render the port incapable of conducting transshipment operations.

Roads: Although road networks generally possess multiple routes and access points to the ports, incapacitating a principal route near a terminal could hinder port operations. MTMC evaluates convoy routes for larger military units which deploy from strategic sea ports. Analysis focuses on obstructions, clearances, and bridge capacity limitations which affords reciprocal benefits for determining the specific, critical roads necessary to support a port's cargo transportation. While the integrity of the entire route is required for uninterrupted movement, bridges present chokepoints which, if destroyed or damaged, would require extensive alternate routing with subsequent delays in deployment schedules.

Aside from the specific routes used for deployment, the security of the general highway and road network serving the port area also presents an important factor in the overall ability of the port to support mobilization and deployment operations. The basic, existing transportation network must remain intact to ensure that all cargo effectively moves to and from the port, and that supporting elements such as employees, contracted labor, repair services, etc. can readily access the port.

Analysis should: (1) describe the road network leading to and from the port/terminal; (2) provide information on the size, composition, condition, and use of primary and alternate

roads; (3) list all bridges on the primary and alternate roads, describing the size, composition, and condition; and (4) identify shortcomings, problems, and potential vulnerabilities.

Railway: Another asset common to all ports involves railways. Outsize cargo (i.e. tanks, helicopters, etc.) generally moves by rail from a military installation to the port. Due to inherent characteristics and basic construction, rail lines are relatively easy to sabotage or destroy. "A small section of missing or misaligned track, or a small switch along the way, can have disastrous consequences, requiring weeks and months for clean-up and repair."[6] An adversary could easily derail military shipments enroute from home installations to ports of embarkation. The consequences, in terms of lost equipment and personnel could seriously impede the deployment schedule. Many ports rely on a single, critical track from the switching station to the terminal. Once a rail line is compromised, rail service is effectively terminated until the line can be repaired or replaced. For the most part, rail lines are accessible, and include isolated and unprotected sections, running through miles of undeveloped, unobserved areas.

Analysis should: (1) describe the rail networks leading to and from the port/terminal; (2) provide information on the number, composition, condition, and use of primary and alternate rails; (3) list all bridges on the primary and alternate rail lines, describing the size, composition, and condition; and (4) identify shortcomings, problems, and potential vulnerabilities.

Personnel: The river pilots of the Cape Fear Pilots Association constitute a critical asset for both MOTSU and the Port of Wilmington. Due to the limited scope of the work and the seven year apprenticeship program, only eight licensed, active pilots provide service on the

Cape Fear River. Because of the numerous bends and turns coupled with the heavy shoaling deposits throughout the entire course of the river, only experienced pilots, familiar with the characteristics of the river, can safely navigate the approach and entrance channels.

All terminals rely on personnel to perform critical functions in support of the port mission. Pilots, stevedores, and longshoremen provide services not found in any other sector of the work force. Analysis should focus on: (1) the name of the organizations and functions performed; (2) the number of organizations and personnel available; (3) affiliations with unions, associations, etc.; (4) background security checks, if any; (5) history of relations (e.g., work stoppages or delays, theft, vandalism, sabotage, etc.); and (6) any noteworthy comments or limitations affecting the port mission.

Pilots: Pilots provide essential services for the safe navigation of channel lanes. All U.S. strategic sea ports require the services of pilots who are trained and licensed to operate in a particular harbor. An accidental or intentional loss of pilots would seriously effect port operations. Ships cannot safely transit channel passages without the services of a pilot.

Stevedores: Stevedores provide support services and equipment necessary to on-load/off-load ships. All U.S. strategic seaports require the use of commercial stevedores.

Longshoremen: Longshoremen provide the labor and expertise necessary to on-load/off-load ocean vessels. Presently, the International Longshoremen's Association (ILA), an independent union organization, provides all longshoremen services for all U.S. strategic seaports.

Facility Support: Terminal administrators hire or contract personnel to perform various port functions. Electricians, crane operators, clerks, road clearing crews, security forces, fire

fighters, mechanics, and others provide critical functions necessary to maintain uninterrupted port operations.

Facilities: The two container cranes located on the South Wharf are critical assets for the Military Ocean Terminal at Sunny Point (MOTSU). The transshipment of containerized ammunition (the port's mission) requires the use of these cranes. The criticality of the cranes increases since there is no identified back up asset capable of replacing the function provided by the container cranes.

General: Facilities analysis focuses on terminal assets and the functions necessary to support deployment operations with respect to receiving, staging, and loading materiel and related cargoes to meet national defense needs.

Material Handling Equipment (MHE): Terminals require specialized equipment (e.g. conveyors, forklifts, dollies, etc.) to on-load/off-load cargo between carriers. Frequently, the location and quantities of MHE dictate the speed at which cargo transfer occurs. The analyst should address the: (1) type of MHE or cargo handling equipment; (2) use; (3) location; (4) quantity; (5) owner (e.g., port, stevedore, leased); (6) resources required to operate the MHE (e.g., fuel, battery, electricity, etc.); (7) storage location and means of securing the MHE; (8) capacity; (9) constraints; and (10) back-up plans.

Cranes: Transshipment operations require extensive use of cranes. The varieties and models of cranes used vary with the type, size, and weight of the cargo (e.g., container cranes, gantry, jib, floating, etc.). Analysis should address the: (1) type of crane; (2) use; (3) location (specify whether they are fixed, mobile, floating, or portable); (4) quantity; (5) owner (e.g., port, stevedore, leased); (6) resources required to operate the crane (e.g. fuel, battery,

electricity, etc.); (7) storage location and means of securing the crane; (8) capacity; (9) constraints; and (10) back-up plans.

Storage Areas: Most ports and terminals possess areas identified for the temporary and/or long-term storage of cargoes. Some of these areas may be located beyond the terminal perimeter and vary in the size, composition and resources available. Analysis should address: (1) the area name; (2) description for both improved and unimproved areas, covered and uncovered storage, warehouses, transit sheds, etc.; (3) location; (4) dimensions; (5) surface composition; (6) access; (7) lighting; (8) existing security measures; (9) ease of providing utilities; (10) capabilities; and (11) constraints.

Marshaling Areas: Military deployments require areas to assemble and organize equipment for loading on vessels. Analysis should address: (1) area name; (2) description for both improved and unimproved areas; (3) location; (4) dimensions; (5) surface composition; (6) access; (7) lighting; (8) existing security measures; (9) ease of providing utilities; (10) capabilities; and (11) constraints.

Marine Repair Facilities: Marine repair facilities do not usually perform a specific function in the transshipment of cargo; rather, they provide a service which enhances port operations when an accident occurs. Each repair facility possesses assets which allow it to perform its primary function. Complete, up-to-date information is required on shipyard facilities and on all firms capable of making marine repairs but lacking dry docking facilities. Information includes the general capabilities of the yard (e.g., hull, engineering, electrical repairs. etc.). Many of the repair facilities possess only limited expertise in certain, specialized areas (e.g.,

plate shop, shaft, propeller, sheet metal, welding, riggers, boilers, carpenter, joiner, foundry, engineering, electrical, coppersmith, machine, forge, engine, pipe, galvanizing, etc.).

Maintenance Facilities: Terminals often have on-site maintenance facilities to ensure uninterrupted port operations (e.g. vehicle, equipment, and real property maintenance). Analysis should address: (1) location; (2) capabilities; (3) hours of operation; (4) owner (e.g. port, contract, lease, etc.); and (5) limitations.

Utility Systems: Utility systems (e.g., water, sewer, refuse removal, etc.) do not normally provide a function necessary for the continued functioning of the terminal in terms of vessel loading, cargo handling, and staging operations. The loss or interruption of any of the major systems, however, would reduce the efficiency of operations and require time and energy to repair or replace the damage. For the most part, utility systems are provided by a single source, with little concern for backup capability, even though they are usually unprotected, and easily accessible. Analysis should describe each utility addressing: (1) source; (2) port requirements; (3) lines provided; (4) capacity; (5) back-up; and (6) constraints.

Electric Power: Electricity is a critical asset for the Military Ocean Terminal at Sunny Point (MOTSU). Safety regulations require the use of electric forklifts when loading ammunition. As such, MOTSU must possess the ability to re-charge forklift batteries in order to continue its ammunition transshipment operation. A total loss of electricity for more than eight hours (i.e. the life of a battery) would prevent MOTSU from loading ships in accordance with the shipping schedule designed to meet the warfighter's required delivery date.

Virtually all ports rely on electricity for daily operations. Lights, computers, office equipment, maintenance facilities, security alarms, battery recharging stations, and other

components of terminal operations require electricity to operate. Most ports do not possess adequate back-up sources of electricity to continue normal port operations.

Many sea ports receive their electricity from a local power generation substation, most of which do not have redundant circuits. It is not difficult to follow the power lines from the port to the substation source. Most substations are located beyond the seaport perimeter and remain unguarded. Targeting the electrical distribution system at the substation is easy and would slow port operations until electricity is restored. Analysis of the electrical power system should describe: (1) the source; (2) the port requirement; (3) the number and type of lines provided; (4) capacity; (5) identified back-ups; and (6) constraints.

Telecommunications: Computers constitute a critical asset for the Port of New York-New Jersey. Virtually all manifests, berthing assignments, and intermodal carrier transactions occur via the computer network. The loss of computer assets would create bottlenecks within the port resulting in delays and an inability to maintain the port throughput commensurate with the required delivery date in an OCONUS theater.

Telephones: Ports and terminals rely on secure and unsecure telephones for normal and crisis communication. Analysis should address identify: (1) the source; (2) the port requirement; (3) the number of lines provided; (4) the existing capacity; (5) identified back-ups; and (6) constraints.

Computers: Port authorities and government officials conduct business transactions, develop manifests, log vessel traffic, etc. using computer technology. Many computer files contain the arrival dates of ships, cargo descriptions, and other sensitive. An adversary could acquire shipping information for subsequent action or they could disable the port's computer

network. Disabling the port's computer network would create bottlenecks and disrupt normal port operations. Computer systems are reachable, the only variables are how much time and resources it takes. Analysis should describe: (1) the number and type of computer networks and work stations; (2) the number of secure networks and work stations; (3) the number of incoming and outgoing lines; (4) the volume of computer traffic coming-in and going-out of the sea port; (5) existing physical and communication security procedures; (6) the frequency and type of viruses, as well as the impact on port operations; (7) identified back-up plans; and (8) constraints.

Adjacent Facilities: The Military Ocean Terminal at Sunny Point (MOTSU) shares a common border with the Brunswick Nuclear Power Plant. An accident at the power plant or an act of sabotage resulting in the release of radioactive fallout material would close the port. While the nuclear power plant is not an asset of the port, the plant's activity directly impacts on the port's ability to perform its mission.

An adversary does not have to directly target a port in order to affect port and terminal operations. Targeting an adjacent facility (i.e. nuclear power plant, petroleum processing plant, chemical manufacturing site, etc.) can create a condition which curtails port operations. A chemical leak into the harbor could prevent the safe passage of ocean vessels (not to mention the environmental clean-up that would cause the rerouting of ship traffic).

Many port and terminal complexes are located in industrial areas. Many businesses conduct the manufacturing of hazardous materials near the port complex. Additionally, businesses which ship their products by ocean vessels frequently own or lease storage facilities within or

near the port. Consequently, many ports contain hazardous materials on railcars, tank farms, and in warehouses.

Analysis should include: (1) the names of all facilities in the port area where an accident could affect port operations; (2) the location and distance from the port; (3) the type of operation; (4) the type of potential hazard; (5) the potential impact on port operations in the event of an accident at the adjacent facility; (6) existing communication with the adjacent facility; (7) the description of physical security measures; and (8) the port contingency plan in the event of adjacent facility crisis which impacts on the port operation.

Summary: The value of the vulnerability assessment is predicated on properly identifying those critical functions necessary to ensure uninterrupted port operations. The analyst's knowledge of intermodal transshipment operations, coupled with a degree of subjectivity, will enhance the prospect of accurately identifying critical functions and assets. A thorough analysis of the port mission, delineating those functions required to accomplish the mission, identifying the assets required to complete the critical functions, and determining critical assets will provide the basis for determining the vulnerability of individual, critical assets. Only an in-depth analysis of all functions, and their interrelationships, will result in a compilation of critical functions and the accurate identification of the critical assets list.

All ports and terminals possess certain common components which are critical for their operations. However, most port authorities and commanders provide redundancy or have the ability to repair damage with limited disruption to the overall port mission. Nevertheless, this common component checklist provides the basis from which a trained analyst can develop a critical assets list. Each critical asset then requires an individual asset vulnerability assessment.

Determining the Vulnerability of Critical Assets

General: The previous steps identified the *critical functions* necessary to accomplish the port mission and identified those *assets* required to complete critical functions. The final step in the port vulnerability assessment involves determining the vulnerability of each *critical asset*. Assets whose vulnerability may be high but do not provide a critical function do not warrant additional analysis. Identifying the vulnerability of critical, individual assets allows commanders or port authorities to take proactive measures to reduce the vulnerability of assets which, in turn, allows the port to continue its primary mission (i.e. the transshipment of cargoes). This section addresses a methodology for determining the vulnerability of critical assets.

Vulnerability Factors:

General: The USCG, U.S. Navy, MTMC, port authorities, and others have vulnerability assessments and physical security checklists to provide a method for determining the relative vulnerability of port facilities. DoD Regulation 5160.54, "Key Asset Protection Program", however, does not provide any specific vulnerability factors, leaving assessment to "the best of the planner's ability."[7] Additionally, the USCG vulnerability factors do not relate to assets and functions (e.g., proximity to international borders, type of port facility, geographic location, etc.).[8]

In order to provide useful information to commanders and port authorities, vulnerability factors must assess the relative vulnerability of an asset. As such, they must focus on the function performed by the asset as it relates to accomplishing the port mission. This study

used the following vulnerability factors: criticality; accessibility; recognizability; effort; recuperability; and existing security measures.[9]

Criticality: Criticality determines how vital the asset is to performing a mission essential function. The criteria used to measure criticality is the percentage of normal operations that can occur without the asset. Back-up assets and contingency plans reduce the criticality of an asset.

Accessibility: Accessibility involves the ease with which an adversary can reach an asset, including direct and remote accessing. The criteria used to measure accessibility is the degree of difficulty associated with reaching the asset.

Recognizability: Recognizability refers the ease with which an adversary can identify an asset during various weather and light conditions. This factor includes signature emissions, site location, and other considerations which facilitate locating an asset. The criteria used to measure recognizability is the range at which the asset can be positively identified.

Effort: Effort refers to the amount of resources required to reduce an asset to the extent which results in the loss of a critical function. This factor considers the time, resources, and expertise required to damage, destroy, or steal an asset. The criteria used to measure effort is the degree of difficulty required to neutralize the asset.

Recuperability: Recuperability refers to the resiliency of an asset to resume operations with minimal disruption to the port operation after an act of sabotage. This factor considers the amount of time required to repair or replace an asset. The criteria used to measure recuperability is the amount of time required to repair or replace the asset.

Security Measures: Security includes all active and passive measures taken to minimize hostile actions against the asset. This factor considers the type of security force, its level of training and equipment used, capabilities, limitations, communication with and availability of back-up forces (federal, state and local law enforcement agencies), surveillance techniques, and other physical security measures. The criteria used to measure the overall effectiveness of the security measures is the percentage of authorized personnel and equipment on-hand, and the method of guarding the asset.

Vulnerability Assessment Worksheet:

General: The critical asset list provides the basis for assessing asset vulnerability. The procedures outlined in Appendix B, Critical Asset Vulnerability Assessment Worksheet, provide a quantitative tool for determining the degree of asset vulnerability.

While a degree of subjectivity occurs in any evaluation of port operations, this study attempts to quantify factors where possible and still retain applicability across the spectrum of asset-types (e.g., transportation, MHE, personnel, etc.). As such, not all of the vulnerability factor criteria apply to all assets (e.g., accessibility to a river pilot by land, air, and water is not critical to eliminating the pilot). Common sense and good judgment, used in conjunction with the worksheet, will significantly aid a prudent analyst in determining critical asset vulnerability.

Procedures: The analyst will complete a separate worksheet for each, individual critical asset, consulting with operations and intelligence personnel, physical security personnel, the facility engineer, and users of the assets, as necessary.

Administrative Data: The analyst will provide all of the required administrative data located at the top of the form: (1) print the name of the unit or organization that owns or

operates the asset (e.g., 1301 Major Port Command); (2) provide the name or title of the asset (e.g., South Wharf Container Crane #1); (3) list the name(s) of the analyst(s) performing the assessment; and (4) include the current date that the assessment was performed.

Asset Data: The asset data provides essential data for use by physical security personnel, operation planning staff, commanders, and other. The analyst will: (1) provide a complete description of the asset (e.g., Berth A, 700 feet long, has a steel sheet pile bulkhead and is constructed of concrete-surfaced solid fill on a concrete relieving platform supported by concrete piles with a 60 foot wide concrete-decked extension); (2) describe the location where the asset operates and its storage location; (3) describe the function performed by the asset (e.g., the terminal tug provides all waterside firefighting capabilities necessary to extinguish and control fires occurring in the wharf area during ammunition transshipment operations; an on-site firefighting tug is required by DoT and DoD regulations when conducting ammunition intermodal transfers); and (4) list the back-up assets available to perform the function accomplished by the principal, critical asset (e.g. emergency electrical power is provided by three 60 Kilowatt, alternating current (AC), diesel operated generators located 100 meters from the battery recharging station, requiring 45 minutes to put into operation; the secondary back-up plan...).

Vulnerability Factor Determination: Using the vulnerability assessment tables provided in Appendix B, the analyst will apply the vulnerability factors to determine the asset vulnerability level. The analyst should assume a worst-case situation when assessing vulnerability and explain the individual ratings in the comments section on the form. After carefully studying the asset and considering all of the criteria explained in the table, the analyst will determine a

numerical value rating based on the asset's criticality, accessibility, recognizability, effort required to neutralize, recuperability, and existing security measures; annotate the results on the worksheet form.

After determining the numerical value rating for each of the vulnerability factors, add the figures together and annotate the sum on the worksheet form. The total point value will determine the asset vulnerability level. The vulnerability level is merely an indicator of relative vulnerability. Absent an adversarial threat, a "high" vulnerability level does not, necessarily, imply imminent disruption to port operations.

Assets with "very low" or "low" vulnerability levels possess acceptable safeguards to ensure uninterrupted port operations. Lower numbers may indicate that commanders or port authorities do not maximize available resources and may wish to consider redistributing resources to reduce the vulnerability of other assets. A vulnerability level of "medium", while acceptable, warrants review by the commander or port authority to ensure they identify actions to ensure uninterrupted operation of the critical function performed by the asset. Assets with "high" or "very high" vulnerability levels do not possess adequate safeguards to ensure uninterrupted port operations. Higher numbers indicate that commanders and port authorities must take prompt action (e.g., obtain back-up assets, adjust security measures, etc.) to minimize the vulnerability of assets performing critical functions.

Summary

U.S. seaports play a vital role in providing warfighters with the supplies and equipment necessary to accomplish their assigned missions. The Mobility Requirements Study (MRS) and the Bottom-Up Review Update (BURU) failed to consider potential vulnerabilities to

U.S. strategic ports and the impact on the ports' ability to achieve the required delivery dates. Port authorities and commanders need to conduct port vulnerability assessments prior to the outbreak of hostilities in order to identify those functions and assets which contribute to successfully accomplishing the port's primary mission, the transshipment of cargoes.

An effective vulnerability assessment provides commanders and port authorities with useful information with which to examine the allocation of resources required to safeguard critical port assets. Vulnerability assessments retain an asset focus and do not factor the current threat analysis into the determination of asset vulnerability. Risk analysis comprises the last component of the port security assessment, melding the input from the threat analysis and the port vulnerability assessment into a useful means of confirming or disproving the MRS and BURU assumptions.

---

[1] U.S. Department of Transportation, United States Coast Guard, Marine Safety Manual; Volume VII, Port Security, (Washington: 1993), 2-3.
[2] Ibid., 2-3.
[3] "Deep Water Ports," Code of Federal Regulations, Title 33--Navigation and Navigable Waters, (Washington: U.S. General Services Administration, National Archives and Records Service, Office of the Federal Register, 1 July 1995), Chap 29, 1502.
[4] U.S. Department of Defense, U.S. Army Engineer District, Wilmington, Port Mobilization Master Plan, Volume I, (Wilmington, NC: Wilmington District ACOE, 1989), D-5-16.
[5] U.S. Department of Transportation, United States Coast Guard, Marine Safety Manual; Volume VII, Port Security, (Washington: 1993), 2-1.
[6] U.S. Department of Defense, U.S. Army Engineer District, Wilmington, Port Mobilization Master Plan, Volume I, (Wilmington, NC: Wilmington District ACOE, 1989), P-2-3(3)b
[7] U.S. Department of Defense, Department of Defense Directive 5160.54, "DoD Key Asset Protection Program," (Washington: 1992), E-2.
[8] U.S. Department of Transportation, United States Coast Guard, Marine Safety Manual; Volume VII, Port Security, (Washington: 1993), 2-2-1.
[9] Survivability is frequently a factor when conducting vulnerability assessments. Most port and terminal assets do not possess built-in survivability measures since they are designed and constructed with minimal concern for intentional acts of sabotage. Moreover, an adversary bent on achieving its hostile aims can overcome most of the survivability measures which would exist at a port. Consequently, this study omits survivability as a vulnerability factor for ports.

Chapter 5

Risk Analysis

General

Risk analysis is the component of a port security assessment which binds the process together. Risk analysis is a tool used to determine the appropriate minimum level of security for assets. The information produced during risk analysis provides the commander or port authority with the necessary information to guard selected *assets* against potential *threats* in an efficient manner. Risk analysis is an on-going activity; a change in the threat level or asset vulnerability warrants a risk analysis review.

Neither the USCG, MTMC, nor the port authorities conduct risk analysis for U.S. strategic ports.[1] Moreover, there is not a single, standardized procedure for conducting risk analysis. The present failure to conduct risk analysis results in an inefficient and random application of security measures. DoD and DoT, in conjunction with the NPRN, need to conduct risk analysis of U.S. domestic seaports in order to minimize the possibility of losing a critical asset to an act of sabotage or terrorism.

A subversive act, tied to a military deployment, could seriously affect the MRC plan or any deployment requiring sealift. Only a thorough port security assessment will identify the threat to, and vulnerability of, critical assets and then determine the minimum level of security required to minimize the risk of loosing a critical function provided by an asset. Risk analysis is an essential component of the port security assessment because of its ability to combine the results of threat analysis and vulnerability assessment into a coherent framework with which to appraise existing security measures.

Among the existing risk analysis methods, the Army model best incorporates threat analysis and vulnerability assessment into its procedures for determining the level of risk for assets. Therefore, it is the best suited approach for inclusion into the recommended systems approach for assessing port security. The Department of the Army authored a pamphlet titled, "Risk Analysis for Army Property".[2] The principal shortcoming with the Army model is that it does not include seaports and terminal assets in its list of assets. Developing additional tables to include seaport and terminal assets would result in an acceptable and useful procedure to conduct risk analysis for seaports.

DoD should direct the Army to create additional tables specifically for seaports and terminals. DoD, DoT, and the National Port Readiness Network (NPRN) should adopt a modified version of the Army procedure for analyzing risk and direct commanders and port authorities to conduct risk analysis for all U.S. strategic seaports.

Risk Analysis Procedure

The following paragraphs describe the Army procedure for conducting risk analysis. Refer to Department of the Army Pamphlet (DA Pam) 190-51, Risk Analysis for Army Property , for a more in-depth discussion of the Army model.

As discussed in the previous chapter, an asset is not necessarily a facility. An asset is a resource which performs a function in the accomplishment of an organization's mission. An asset *may* be an individual, facility, piece of equipment, or some other item. Security is focused on protecting assets rather than facilities. Risk involves both, "the impact of the compromise of an asset (vulnerability) and the potential for it being compromised (threat)."[3]

The value of an asset (asset value) and the likelihood that an adversary will target the asset (likelihood) comprise the two factors associated with risk. Asset value is a risk factor which indicates the value or importance of the asset to the organization which owns, controls, or uses the asset. The risk level increases with the criticality or value of the asset. The vulnerability assessment determines the asset value.

The likelihood of an attack, is the second risk factor which, "indicates the attractiveness of the asset to an adversary and the likelihood that an adversary would attempt to compromise the asset."[4] Threat analysis identifies potential or likely adversaries or aggressors who may wish to target an asset. Risk analysis considers each potential aggressor category (e.g., foreign intelligence services (FIS), foreign sponsored terrorists, domestic terrorists or extremists, criminals, protesters, groups or individuals) likely to target a particular asset. The level of risk increases with the likelihood of aggression. An up-to-date, current threat analysis determines the likelihood of a hostile act directed against an asset.

After determining the asset value and likelihood of attack, the analyst identifies the overall risk level of the asset. Risk levels range from I-III; however, the Army does not explain the significance of the various levels (this is another aspect of the Army model requiring modification).

The final step in the Army procedure is to adjust security measures presently allocated to the asset. For example, the risk level of an unsecure, critical wharf (i.e. high vulnerability) with a known, hostile group operating in the port area and capable of targeting the port (i.e. high threat), could result in a high risk level. However, if the commander or port authority

placed an armed guard physically on the asset, the likelihood that a threat group would target the asset is lessened and thus, the risk level decreases.

Summary

Risk analysis is the final step in the vulnerability assessment. Risk incorporates identified vulnerabilities and the current threat condition to determine the overall risk associated with port or terminal assets. Based on the complete port security assessment, commanders are better able to take proactive measures to minimize potential criminal acts and its impact on port operations.

Risk analysis allows commanders and port authorities to safeguard critical *assets* against potential *threats* in an efficient manner. While the U.S. Army model of risk analysis does not specifically identify seaport or terminal assets, it does, nevertheless, provide a quantitative method for assessing risk. Minimal modification to the Army model would readily lend itself to analyzing risk for seaports and terminals.

DoD must take a lead role in safeguarding our nation's vital infrastructure against potential acts of sabotage and terrorism. The ability to deploy and sustain our armed forces in an OCONUS theater of operations relies on U.S. domestic seaports. Risk analysis, properly conducted, allows commanders and port authorities to respond in advance of a potential attack against the port and to ensure uninterrupted port operations.

---

[1] Personal and telephonic interviews with USCG COTPs, MTMC port commanders, and port authorities revealed that risk assessment is not conducted for U.S. strategic ports. The Security Program Manager at Headquarters, MTMC stated in a personal interview on 12 APR 96 at HQ, MTMC, that he does not possess any risk assessment files on U.S. strategic ports and does not believe that any were recently conducted.

[2] U.S. Department of Defense, Headquarters, U.S. Army, "DA Pamphlet 190-51," Risk Analysis for Army Property, (Washington: 1993), i.

[3] Ibid., 1.

[4] Ibid., 1.

Chapter 6

Recommendations

Single Proponent

The Code of Federal Regulations and MOU on Port Readiness should assign overall responsibility for all aspects of port and terminal security, during peace and in times of national defense emergencies, to the U.S. Coast Guard. The Captain of the Port (COTP) presently plays a lead role in security, his/her authority should extend in encompass landward security.

Systems Approach to Assessing Port Security

DoD and DoT should adopt a systems approach to assessing security of strategic seaports. The NPRN should direct the USCG, in coordination with other agencies, to conduct port security assessments for all U.S. strategic seaports. The USCG should retain complete and up-to-date assessments on file and provide copies to responsible agencies with the requisite security clearances.

Threat Analysis

DoT, in coordination with DoD and the NPRN, should direct the USCG Intelligence Coordination Center (ICC) to develop, implement, maintain, and disseminate a port-specific threat analysis. The ICC and NPRN should improve their coordination and communication with the FBI in order to maximize existing intelligence sources. The prompt and continuing dissemination and exchange of information will assist in maintaining effective port security procedures and will enable agencies and operators to adjust their procedures in response to changing conditions and specific threats.

Vulnerability Assessment

DoD and DoT need to adopt standard vulnerability assessments specifically designed to determine critical functions necessary to accomplish the port mission, identify those assets required to complete critical functions, and then determine the vulnerability of each critical asset. DoD and DoT should adopt the method described in this research and conduct vulnerability assessments for all strategic seaports.

Risk Analysis

DoD should direct the U.S. Army to create additional criteria with which to analyze the risk of seaports and terminals. DoD, DoT, and the NPRN should adopt an amended version (i.e. one that includes criteria to evaluate the risk of seaports and explains the risk levels) of the Army model for analyzing risk and direct COTPs, port commanders, and port authorities to conduct risk analysis for all U.S. strategic seaports.

Additional Research

Given the inherent vulnerabilities of the ports, additional research is needed to determine whether the risks warrant the costs associated with implementing improved port security measures. Research is also warranted in the area of recovery planning.

Chapter 7

Conclusion

The recent bombings of the Federal Building in Oklahoma City and of the World Trade Center in New York City demonstrate the vulnerability of the U.S. to acts of terrorism. Hostile threats to our defense infrastructure are a potential reality which cannot be dismissed lightly. The threat may develop from internal, domestic organizations who are disaffected with the political situation or from foreign terrorist organizations who are eager to export their campaigns to the U.S.

In 1988, Oliver Revell, executive Assistant Director for the FBI, told a Senate Subcommittee that, "it is unrealistic to assume that we have the ability or resources to guarantee protection to our nation's infrastructure from every conceivable terrorist attack."[1] The United States remains a free and open society. Virtually anyone can obtain weapons, explosives, and other materials to achieve their hostile aims. Although the use of terrorism has not significantly altered the course of past wars, its use in low and mid-intensity conflicts has caused changes in the ways in which the conflicts were conducted. It is conceivable that terrorist or extremist organizations could hinder our ability to deploy and sustain our forces while engaged in a major regional contingency operation.

There is a danger in using Desert Storm as the defining moment for future deployments. The U.S. must understand that Desert Storm was unique in its duration, limited scope, and ability to foster favorable world opinion. U.S. Strategic and operational commanders must now plan to dominate the entire spectrum of the conflict, from "fort to foxhole" and avoid the false sense of security at home and on the seas.

As resources continue to decline and the operational tempo of the Armed Forces remains high, the necessity of CONUS infrastructure assets will increase in importance as force multipliers. DoD's *assumption* that, "there will be no degradation in our strategic delivery capabilities because of [hostile] actions...[or] damage to ports" begs further analysis.[2] Mobility and logistics planners should prove or disprove the validity of their assumptions or potentially fall prey to the consequences of misguided planning.

A systems approach to assessing port security will confirm or deny the DoD mobility requirements study's assumption concerning the ports' ability to provide sustainment operations without degradation due to hostile acts. A systems approach provides the information required to determine the likelihood of threat activity against a port, the critical assets needed to accomplish functions necessary to maintain port operations, and the risk associated with existing security measures. Security assessments conducted on all U.S. strategic ports will identify efficient alternatives to alleviate the criticality of any single asset, thereby enhancing overall port security and the ports' ability to provide critical cargoes to theater CINCs.

The ability to fight and win is dependent on the effectiveness with which U.S. forces are projected in any theater of conflict. History demonstrates the critical role our ports play in supplying a credible deterrent force. The goal of future mobility planning must ensure that our ports remain open and unencumbered in providing supplies and equipment whenever and wherever needed. The possibility that a single, violent act can shatter the time-sensitive deployment schedule demands a new sense of awareness and vigilance on the part of DoD.

---

[1] Oliver B. Revell, III, Statement, U.S. Congress, Senate Subcommittee on Judiciary, Terrorist Attacks Against the United States, Hearings, (Washington: The U.S. Govt. Print. Offc., 1990), 5.

[2] U.S. Department of Defense, Joint Chiefs of Staff, Mobility Requirements Study, Bottom-Up Review Update, (Washington: 1995), IV-A-5.

Appendix A

Vulnerability Assessment Outline

I. Administrative Data:

A. *Name of asset*: (i.e. legal name of asset) Also indicate name of parent organization, if applicable.

B. *Location*:
1. *Mailing Address*: Complete mailing address, including nine digit zip code.
2. *Physical Location*: If the asset does not have a street address or if the mailing address is different from the physical location, describe the latter (e.g., Route 1, Smithfield, VA, three miles south of Smithfield on Interstate 66. On Grog Road, turn north 1.5 miles to facility).
3. *County*: County where asset is physically located.

C. *Geographical Coordinates*: Express in degrees (o), minutes ('), and seconds (") to the nearest ten seconds for latitude and longitude. Coordinates should refer to the geographic center of the surveyed asset. The facility engineer can provide this information.

D. *Assessment Team Personnel*:
1. *Agency*: Identify the agency conducting the vulnerability assessment.
2. *Personnel*:
   a. List the names of the personnel conducting the assessment.
   b. Did Army Corps of Engineer or USCG representatives participate in the assessment?

II. Specific Information: Provide a narrative description covering the following information:

A. *Geographical Location*: Describe the geographic area and terrain surrounding the port and adjacent areas (e.g., rural, urban, industrial, population density, mountainous, hilly, rolling, level, etc.).

B. *Physical Profile of the Port*: Describe the principal structures the port complex. Include comments on entry and exit points (pedestrian, road, rail, air, water).

C. *Port Mission Statement*.

D. *Critical Functions*: Describe the critical functions required to accomplish the port mission.

E. *Physical Security Plan*: Describe the existing physical security plan.
1. *Security Force*:
   a. Type (e.g., contract, sworn, armed/unarmed).
   b. Level of training.
   c. Authorized strength.

d. Authorized equipment (e.g., weapons, night vision devices, chemical protective masks, communication, vehicles, etc.).

e. Other considerations addressing the security force.

2. *Security Operations*:

a. Method of guarding the site (e.g., gates, asset protection, patrols, waterside, shoreside, etc.).

b. Access controls (e.g., identification, inspections, etc.).

c. Early warning and anti-intrusion measures.

d. Electronic monitoring devices.

e. Other noteworthy aspects of the port security operation.

3. *Crime Prevention*:

a. Perimeter fence.

b. Lighting.

c. Inspections.

d. Other aspects of the crime prevention program pertinent to port security operations.

4. *Communication*:

a. Communication with federal, state and local law enforcement agencies (e.g., existing agreements, response times, capabilities, etc.).

b. Communication with facilities adjacent to the port (e.g., existing agreements, alert and notification procedures, etc.).

c. Means of receiving current threat analysis, intelligence summaries, early warning, etc.

F. *Port Component Analysis*:

1. *Harbor*:

a. Harbor Data.

b. Harbor Works.

c. Depths.

d. Basins.

e. Channels.

f. Anchorages.

g. Other pertinent information.

2. *Port*:

a. Port Data.

b. Principal activities performed by terminals.

c. Capacity.

d. Approach channels.

e. Hydrographic conditions.

f. Geophysical conditions.

g. Other pertinent information.

3. *Terminal*:

a. Terminal data.

b. Principal activities.

c. Capacity.

d. Access.

e. Other pertinent information.

4. *Wharf*:
   a. Use.
   b. Location.
   c. Construction.
   d. Dimensions.
   e. Capacity.
   f. Constraints and shortcomings.
   g. Other pertinent information.
5. *Transportation system*:
   a. Road.
   b. Rail.
   c. Any other mode of transportation used to accomplish the port mission.
6. *Personnel*:
   a. Pilots.
   b. Stevedores.
   c. Longshoremen.
   d. Facility support personnel.
   e. Other critical personnel.
7. *Facilities*:
   a. Material handling equipment (MHE).
   b. Cranes.
   c. Storage facilities.
   d. Marshaling areas.
   e. Marine Repair.
   g. Maintenance facilities.
   h. Other facilities required to accomplish the port mission.
8. *Utility systems*:
   a. Utility .
   b. Source.
   c. Port/terminal requirements.
   d. Lines provided.
   e. Capacity.
   f. Back-up.
   g. Other pertinent information.
9. *Electric power*:
   a. Source.
   b. Port/terminal requirements.
   c. Lines provided.
   d. Capacity.
   e. Back-up.
   f. Other pertinent information.
11. *Telecommunications*:
   a. Telephones.
   b. Computers.
   c. Other telecommunication nodes necessary to conduct port operations.

12. *Particular susceptibilities*:
    a. Mining.
    b. Deception.
    c. Other susceptibilities unique to the port.

G. *Critical Assets*: Identify the port's critical assets; compile the critical assets list.

H. *Contingency Plans*: Describe contingency plans and identified back-up assets to ensure uninterrupted port operations, focus on critical assets.

I. *Critical Asset Vulnerability Assessment Worksheets*: Include completed critical asset vulnerability assessment worksheets on all critical assets (see Appendix B).

J. *Summary*:
1. *Recommendations.*
2. *Summary.*

Appendix B
Critical Asset Vulnerability Assessment Worksheet

General: Not all assets possess the same degree of vulnerability. Assets which provide a critical function in support of the unit's mission may present a greater degree of vulnerability to successfully accomplishing the port mission. A variety of factors determine the overall vulnerability of an asset. The vulnerability assessment worksheet identifies potential shortcomings within a port's operation. Asset vulnerability identification allows a commander or port authority to take proactive measures to reduce the vulnerability of assets which, in turn, allows critical functions to occur in support of the port's primary mission, the transshipment of cargo.

This worksheet is primarily concerned with the emergency deployment of military units and equipment from their peacetime locations to designated surface ports of embarkation (SPOE) to meet the required delivery date (RDD) in a theater of operations. As such, time plays a critical role in accomplishing the port mission and is a primary consideration in the vulnerability assessment.

Vulnerability Assessment Worksheet Procedure: The following procedure applies to all assets which perform a critical function in support of the port mission. Consult with operations and intelligence personnel, physical security personnel, facility engineers, and users of the assets, as necessary, when conducting this assessment.

The analyst should assume a worst-case situation when assessing asset vulnerability and explain individual ratings in the comments section of the form. Assuming the worst-case serves to highlight vulnerabilities and affords commanders and port authorities the opportunity to analyze the adequacy of resources dedicated to safeguarding assets. See Figure 1, DX Form XXXX-R (Vulnerability Assessment Worksheet).

Step 1: Identify the unit or organization that uses the asset. Provide the asset title or name. Include the name of the analyst performing the assessment and the current date. Enter this information in the spaces provided on the DX Form XXXX-R. See Figure 2, A Completed DX Form XXXX-R (Vulnerability Assessment Worksheet).

Step 2: Describe the asset. List the dimensions, weight, sub-components (if any), construction, composition, and other descriptive remarks.

Step 3: Provide the location of the asset. Include both the operational and storage locations.

Step 4: Describe the function performed by the asset. Provide comments concerning the asset's importance in accomplishing a particular function as part of the overall port operation.

Step 5: State whether or not contingencies exist to restore operations in the event of asset loss. List alternative assets and contingency plans to allow the unit or organization to continue its mission. Mention the extent to which degraded operations can occur without the asset. Back-up assets will reduce the relative vulnerability of an asset.

Step 6: Complete the asset assessment procedure using the vulnerability factor tables found at the end of this appendix:

(1) Select the applicable vulnerability factor table.

(2) Select the entry from each rating table which most closely applies to the asset; assume a worst case situation and select the highest vulnerability factor value rating.

(3) Record the numerical values in the space provided on DX Form XXXX-R.

Criticality: This factor assesses the criticality of an asset in the overall accomplishment of an essential function required to accomplish the unit's mission. The criteria used to measure criticality is the percentage of normal operations that can occur without the asset. Evaluate this factor using Table 1.

Accessibility: This factor assesses the relative ease with which a target is reached, either directly or indirectly (e.g., entering an electrical substation vs. entering the computer network). The criteria used to measure accessibility is the degree of difficulty associated with reaching the asset. Evaluate this factor using Table 2.

Recognizability: This factor assesses the degree to which the target is recognizable under varying weather, light, and seasonal conditions without confusion with other targets or components. The criteria used to measure recognizability is the range at which the asset can be positively identified. Evaluate this factor using table 3.

Effort: This factor assesses the amount resources (e.g. knowledge, skill, abilities, material, time, etc.) required to damage, destroy, or steal an asset to the extent that the asset cannot perform its critical function. The criteria used to measure effort is the degree of difficulty required to neutralize the asset. Evaluate this factor using Table 4.

Recuperability: This factor assesses the resiliency of an asset to resume normal operation of a critical function with minimal delay or disruption. The criteria used to measure this factor is the amount of time required to repair or replace the asset. Evaluate this factor using Table 5.

Security Measures: This factor assesses the existing security measures to prevent illegal access to an asset, to detect unauthorized access, and to mitigate the threat. The criteria used to evaluate this factor is the percentage of authorized personnel and equipment on-hand, and the method of guarding the asset. Evaluate this factor using Table 6.

Step 7: Add the numerical values for each of the six vulnerability factors and annotate in the appropriate box on DX Form XXXX-R.

Step 8: Compare the sum with the ranges of sums in Table 7. Determine the overall vulnerability level for the asset and annotate on DX Form XXXX-R.

Step 9: Provide comments on vulnerability factors which were rated 4 or 5, or any other noteworthy information. These comments will allow commanders to identify specific weaknesses and take remedial action.

Step 10: Include vulnerability assessment worksheets for all critical assets within the port. Include all complete worksheets with the port vulnerability assessment (see Appendix A, Vulnerability Assessment Outline).

Vulnerability Rating Explanation: The vulnerability level is merely an indicator of relative vulnerability. Absent a current threat analysis, the vulnerability level only signals potential adequacy, acceptability , or inadequacy with existing safeguards. A "high" vulnerability level does not, necessarily, imply imminent disruption to port operations.

Assets with "very low" or "low" vulnerability levels possess acceptable safeguards to ensure uninterrupted port operations. Lower numbers may indicate that commanders or port authorities do not maximize available resources and may consider redistributing resources to reduce the vulnerability of other assets. The distinction between "low" and "very low" relates to the accuracy of identifying critical assets and the efficient use of resources. A vulnerability level of "medium", while acceptable, warrants review by the commander or port authority to ensure they identify actions to ensure uninterrupted operation of the critical function performed by the asset. Assets with "high" or "very high" vulnerability levels do not possess adequate safeguards to ensure uninterrupted port operations. Higher numbers indicate that commanders and port authorities must take prompt action (e.g., obtain back-up assets, adjust security measures, etc.) to minimize the vulnerability of assets performing critical functions. The distinction between "high" and "very high" relates to the urgency with which commanders must act to safeguard a critical function.

Critical Asset Vulnerability Assessment Worksheet Tables

Table 1

Criticality	Value Rating
Asset is mission critical; asset's loss prevents the unit from conducting its mission; no back-up is identified or available	5
Asset is mission critical; degraded operations (i.e. less than 50% of original output) until the asset is repaired or replaced; no back-up is identified or available	4
Asset's loss has significant impact on unit mission; degraded operations (i.e. 51-75% of original output) until the asset is repaired or replaced; back-up is available but requires time to replace (i.e. greater than 12 hours)	3
Asset's loss has significant impact on unit mission; degraded operations (i.e. 76-99% of original output) until the asset is repaired or replaced; back-up is available; normal operations will resume within 12 hours	2
Asset's loss has minor impact on unit mission; unit can perform its mission function with minimal adjustment; or back-up is immediately available (i.e. less than 1 hour)	1
Asset's loss would have negligible impact on unit mission; unit can continue mission function with minimal disruption	0

Table 2

Accessibility	Value Rating
Easily accessible (ingress and egress) by land, air, and water (multiple routes available); no obstacles; asset is in the open or near the perimeter; no security measures; OR the asset is reachable without accessing the facility site; asset can be targeted from a remote site	5
Asset is accessible by land, water, or air (multiple routes available); minimal obstacles to gaining access (e.g. fence only); asset is in the open; minimal security measures	4
Asset is accessible by land, water, or air with adequate planning (multiple routes available); several obstacles to overcome to reach the asset; asset is well within the perimeter; limited security measures (i.e. lights, patrols, no electronic measures)	3
Limited number of routes available to gain access to the asset; numerous obstacles to overcome; asset is location is difficult to reach; medium level security measures (i.e. lights, patrols, some electronic measures)	2
Not readily accessible by land, air, or water; requires extensive planning and resources to gain access; numerous obstacles to overcome; asset is location is difficult to reach; medium to high level of security (i.e. lights, patrols, early warning and anti-intrusion devises)	1
Extremely difficult to gain access; numerous natural and manmade obstacles to overcome; high level security with manned guards on the asset	0

Table 3

Recognizability	Value Rating
Asset projects a large signature (e.g. lights, sound, & smell); readily identifiable during all light, weather, and seasonal conditions, and at long ranges; located in a large built-up area	5
Asset projects a large signature (e.g. lights & sound); identifiable during day and night, and at long ranges; located in built-up area	4
Asset projects a medium signature (e.g. lights or sound); readily identifiable during day but only recognizable close range (within 500 meters) at night; located in urban or suburban area	3
Asset projects a low signature (e.g. low levels of light or sound); readily recognizable in daylight but only identifiable within 100 meters at night; located in rural area	2
Asset does not emit a signature; recognizable in the daylight only; remote site	1
Asset does not emit a signature; asset is hidden and blends in with the surrounding vegetation; remote site; not recognizable	0

Table 4

Effort	Value Rating
Asset is easily damaged; requires little skill, few resources, and minimal time; no precautionary measures exist to prevent intentional damage	5
Asset is not complex; requires limited knowledge, skills, and abilities to neutralize; requires few resources and little time to destroy, damage or steal the asset; no existing countermeasures	4
Asset is not complex; requires some knowledge and training; requires limited time and resources to destroy, damage, or steal the asset; existing countermeasures can be easily overcome	3
Relatively complicated asset; requires knowledge, skills, and abilities to properly neutralize the asset; requires a significant amount of time and resources to destroy, damage, or steal the asset; some countermeasures require time to overcome	2
Large or complicated asset; hardened to prevent damage; requires extensive knowledge, skills, and abilities to destroy, damage, or steal the asset; complicated countermeasures	1
Large or complicated asset; difficult to damage; hardened site to prevent damage; virtually unimpenetrable or prone to sabotage	0

Table 5

Recuperability	Value Rating
Asset must be replaced; destruction or damage results in the loss of the function (i.e. greater than 72 hours)	5
Asset can be repaired or replaced, requiring more than 24 hours after occurrence	4
Asset can be repaired or replaced within 12-24 hours of occurrence	3
Asset can be repaired or replaced in less than 12 hours of occurrence	2
Asset can be repaired or replaced within 6 hours of damage	1
Asset is easily repaired or replaced with no loss in operational function (i.e. less than 1 hour)	0

Table 6

Security Measures	Value Rating
No security measures for the asset (fence, lights, and gate guards)	5
Unarmed contract security element; conducts routine patrols and *observation check* of asset	4
Sworn and armed security force, less than *80%* of authorized personnel and equipment present; No electronic surveillance or early warning; conducts routine patrols and *observation check* of asset	3
Sworn and armed security force, less than *95%* of authorized personnel and equipment present; no electronic surveillance or early warning; conducts routine patrols and *physical checks* of assets	2
Sworn and armed security force at *100%* authorized strength and equipment; asset has electronic surveillance, anti-intrusion, or early warning devices; conducts hourly manned *physical check* of asset	1
Sworn and armed security force at 100% authorized strength and equipment; asset has electronic surveillance, anti-intrusion, or early warning devices; asset is *manned and guarded*	0

Table 7

Sum of Value Rating Factors	Vulnerability Rating
0-5	Very Low (VL)
6-11	Low (L)
12-17	Medium (M)
18-23	High (H)
24-30	Very High (VH)

UNIT OF ORGANIZATION _____ DATE _____

ASSET TITLE OR NAME _____ ANALYST _____

Description: _____

Location: _____

Function: _____

Alternatives / Back-Up: _____

Vulnerability Factors	Table Score	Total	Vulnerability Level	Comments (Mandatory for VA Factors of 4 or 5)
Criticality (Table 1)				
Accessibility (Table 2)				
Recognizability (Table 3)				
Effort (Table 4)				
Recuperability (Table 5)				
Security Measures (Table 6)				
Total				
Vulnerability Level (Table 7)				

DX FORM XXXX-R, MAY 96 VULNERABILITY ASSESSMENT WORKSHEET

Figure 1 Example of a Vulnerability Assessment Worksheet; DX Form XXXX-R

UNIT OF ORGANIZATION 1303 MAJOR PORT COMMAND DATE 28 MAY 96

ASSET TITLE OR NAME BERTH A ANALYST MAJ GROHOSKI

Description: 700 feet long, has a steel sheet pile bulkhead and is constructed of concrete-surfaced solid fill on a concrete relieving platform supported by concrete piles with a 60 ft. concrete-decked extension

Location: South wharf; southern-most berth

Function: Wharf Operations 1
Principal berth used outload tracked vehicles
One of only two berths with a RO/RO ramp

Alternatives / Back-Up:
(1) Berth C on North Wharf
(2) Marine Terminal, 3 miles up river has 2 RO/RO berths

Vulnerability Factors	Table Score	Total	Vulnerability Level	Comments (Mandatory for VA Factors of 4 or 5)
Criticality (Table 1)	4			1) Port can't conduct RO-RO at full capacity only 40%
Accessibility (Table 2)	1			2) Early Warning on berth & ramp
Recognizability (Table 3)	4			3) Lights on berth
Effort (Table 4)	1			4) Berth is concrete & steel; Ramp is steel
Recuperability (Table 5)	5			5) If destroyed, gtr than 72 hours to repair
Security Measures (Table 6)	1			6) TV camera on ramp & berth
Total		16		
Vulnerability Level (Table 7)			M	

DX FORM XXXX-R, MAY 96 VULNERABILITY ASSESSMENT WORKSHEET

Figure2 Example of a Vulnerability Assessment Worksheet; DX Form XXXX-R

Selected Bibliography

Books and Articles

Bird, James. Seaports and Seaport terminals. London: Hutchinson & CO, LTD, 1971.

"Cuban Special Forces Prepare for U.S. Attack." Jane's Defense Weekly. 6 March 1996, 3.

Smith, Brent L. Terrorism in America: Pipe Bombs and Pipe Dreams. New York: SUNY Press, 1994.

Department of Defense Publications

Department of the Army. DA Pamphlet 190-51. Risk Analysis for Army Property. Washington: 1993.

Department of the Army. U.S. Army Engineer District, Wilmington. Port Mobilization Master Plan, Volume I. Wilmington, NC: Wilmington District ACOE, 1989.

Department of the Navy. Study of Worldwide Port Facilities. NWC Technical Publication 5062. China Lake, CA: Naval Weapons Center, 1974.

U.S. Department of Defense. DoD Regulation 5160.54. Key Asset Protection Program. Washington: 1992.

U.S. Department of Defense. Report on the Bottom-Up Review. Washington: 1993.

U.S. Office of the Joint Chiefs of Staff. Mobility requirements Study, Bottom-Up Review Update. (Washington: 1995.

Department of Transportation Publications

U.S. Department of Transportation. Maritime Administration. Port Emergency Operations Handbook for Federal Port Controllers. Washington: 1992.

U.S. Department of Transportation. United States Coast Guard. Marine Safety Manual; Volume VII, Port Security. Washington: 1993.

U.S. Government Documents

A National Security Strategy of Engagement and Enlargement. Washington: 1995.

Code of Federal Regulations, title 33--Navigation and Navigable Waters. Washington: 1995.

U.S. Congress. Senate. Committee on Judiciary. Terrorist Attacks Against the United States. Hearings. Washington: 1990.

U.S. President. Executive Order. "Assignment of Emergency Preparedness Responsibilities, 1988." Codification of Presidential Proclamations and Executive Orders, April 13, 1945-January 20, 1989. Washington: 1989, 887-911.

Unpublished Papers

McDonald, William and Arnold Snowberger. "Analysis of Seaports and Their Vulnerabilities to Interdiction." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1984.

Interviews

Interview with Captain John Reinke, NY-NJ Port Police, Elizabeth, NJ: 19 March 1996.

Interview with Captain John Rice, USCG, Captain of the Port, Wilmington, NC: 10 April 1996.

Interview with Captain T. H. Gilmour, USCG, Captain of the Port, Governors Island, NY: 18 March 1996.

Interview with Colonel Waldemar Carmona, U.S. Army, Commander, Military Ocean Terminal, Bayonne, NJ: 18 March 1996.

Interview with LT Karl DeLoof, USCG, MSO Wilmington, NC: 10 April 1996.

Interview with Mr. Joseph Kass, Deputy Chief of Staff for Intelligence, MTMC Eastern Area Command, Bayonne, NJ: 20 March 1996.

Interview with Colonel C. Parker, Commander, Military Ocean Terminal, Sunny Point, NC: 12 April 1996.

Interview with Mr. Robert Jones, HQ, MTMC, Security Program Manager, Falls Church, VA: 16 April 1996.